7

Bridge/Router Internetworking Protocols

There are a number of additional protocols which are generally used for bridge/router internetworking. These protocols are located in the Data Link Layer, and may carry encapsulated protocols in higher layers, e.g., IP, IPX, Ethernet and Token Ring.

The following bridge/router protocols are described in this book:

- Cisco Router.
- Cisco SRB.
- Cisco ISL.
- Cisco DRiP.
- CDP: Cisco Discovery Protocol.
- DISL: Dynamic Inter-Switch Link Protocol.
- VTP: VLAN Trunk Protocol.
- RND.
- Wellfleet SRB.

- Wellfleet BOFL.
- BPDU.
- PPP including PPP Multilink, LCP, LQR, PAP, CHAP, IPCP, IPXCP, ATCP, BAP, BACP, BCP, PPP-BPDU, CCP, IPv6CP, SNACP, BVCP, NBFCP, DNCP, L2F, L2TP, ECP, OSINLCP, PPTP, and SDCP (refer to Chapter 23).
- Frame Relay (refer to Chapter 11).
- Cascade (refer to Chapter 11).
- Timeplex (BRE2) (refer to Chapter 11).
- IP over X.25 (refer to Chapter 28).
- SMDS/DXI (refer to Chapter 24).

Cisco Router

The Cisco company produces communications equipment such as routers and bridges which use a proprietary protocol header (known as Cisco Router) to transfer LAN protocols via WAN.

Cisco Router's default encapsulation on synchronous serial lines uses HDLC framing with packet contents as defined in the following illustration:

Address	Control	Protocol code	Information
1 byte	1 byte	2 bytes	variable

Cisco router header structure

Address

Specifies the type of packet:
0x0F Unicast packets.
0x8F Broadcast packets.

Control

Always set to zero.

Protocol code

Specifies the encapsulated protocol. The Protocol Code is usually Ethernet type codes; however, Cisco has added some codes to support packet types that do not appear in Ethernet.
Standard Ethernet values include:
0x0200 PUP.
0x0600 XNS.
0x0800 IP.
0x0804 Chaos.
0x0806 ARP.
0x0BAD Vines IP.
0x0BAF Vines Echo.
0x6003 DECnet phase IV.
0x8019 Apollo domain.
0x8035 Cisco SLARP.
0x8038 DEC bridge spanning tree protocol.
0x809B Apple EtherTalk.
0x80F3 AppleTalk ARP.

0x8137 Novell IPX.
Cisco-specific values include:
0x0808 Frame Relay ARP.
0x4242 IEEE bridge spanning protocol.
0x6558 Bridged Ethernet/802.3 packet.
0xFEFE ISO CLNP/ISO ES-IS DSAP/SSAP.

Information

Higher-level protocol data.

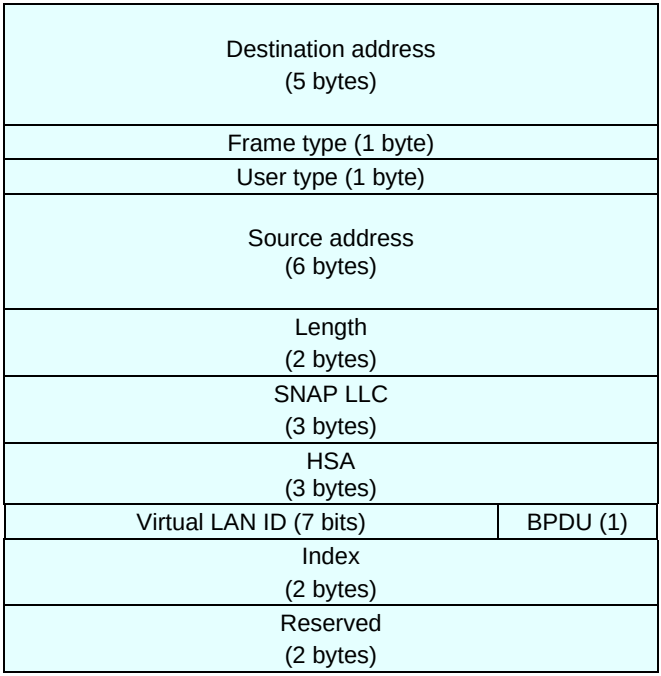
Cisco SRB

Cisco uses a proprietary header in order to pass Token Ring information over WAN lines. This is known as Source Routing Bridging (SRB).

Cisco ISL

The Inter-Switch Link or ISL is used to inter-connect two VLAN capable Ethernet switches using the Ethernet MAC and Ethernet media. The packets on the ISL link contain a standard Ethernet, FDDI, or Token Ring frame and the VLAN information associated with that frame. Some additional information is also present in the frame.

The format of the header is shown in the following illustration:



Cisco router header structure

Destination address

The destination address field contains a 5 byte destination address.

Frame type
The frame type indicates the type of frame that is encapsulated. In the future this could be used to indicate alternative encapsulations. The following Type codes are defined:
0000 Ethernet
0001 Token Ring
0010 FDDI
0011 ATM

User type
0 Normal priority.
1 Highest priority.

Source address
Source address of the ISL packet. It should be set to the 802.3 MAC address of the switch port transmitting the frame. It is a 48 bit value.

Length
A 16-bit field containing the length of the packet in bytes, not including the DA, T, U, SA, LEN and CRC fields. The total length of the fields excluded is 18 bytes so the length field is the total length minus 18 bytes.

HSA
High bits of source address field. Contains the upper 3 bytes of the SA field.

Virtual LAN ID
This is the virtual LAN ID of the packet. It is a 15-bit value that is used to distinguish frames on different VLANs. This field is often referred to as the color of the packet.

BPDU and CDP indicator
0 Not forwarded to the CPU for processing.
1 Forwarded to the CPU for processing.

Index
The index field indicates the port index of the source of the packet as it exits the switch. It is used for diagnostic purposes only and may be set to any value by other devices. It is a 16-bit value and ignored in received packets.

Reserved
A reserved field.

DRiP

Cisco Ios Release 11.3(4)T

The Cisco Duplicate Ring Protocol (DRiP) runs on Cisco routers and switches that support VLAN networking and is used to identify active Token Ring VLANs. A VLAN is a logical group of LAN segments with a common set of requirements. DRiP information is used for all-routes explorer filtering and detecting the configuration of duplicate TrCRFs, across routers and switches, which would cause a TrCRF (Token ring Concentrator Relay Function: a logical grouping of ports) to be distributed across ISL trunks. DRiP sends advertisements to a multicast address so the advertisements are received by all neighboring devices. The advertisement includes VLAN information for the source device only. The DRiP database in the router is initialized when TRISL (Cisco's Token ring Inter-Switch Link) encapsulation is configured, at least one TrBRF (Token ring Bridge Relay Function: a logical grouping of TrCRFs) is defined and the interface is configured for SRB (Source Route Bridging) or for routing with RIF.

When a switch receives a DRiP advertisement from a router, it compares the information in the advertisement with its local configuration to determine which TrCRFs have active ports and then denies any configuration that would allow a TrCRF that is already active on another box to be configured on the local switch. If there is a conflict between 2 identical TrCRFs, all ports attached to the conflicting TrCRFs are shut down in the switches and the router's ports remain active. A DRiP advertisement is sent every 30 seconds by the router.

DRiP is assigned the Cisco HDLC protocol type value 0x0102. A Cisco proprietary SNAP value is used. The following fields appear in the structure:

Version
The version number.

Code
The code number.

VLAN info count
The number of VLAN information elements.

VLAN 1... VLAN2...
Various VLAN information elements.

CDP

The Cisco Discovery Protocol (CDP) is a protocol for discovering devices on a network. Each CDP-compatible device sends periodic messages to a well-known multicast address. Devices discover each other by listening at that address.

CDP operation can be enabled or disabled on the FastHub through the object cdpInterfaceEnable. When enabled, the network management module (NMM) SNMP agent discovers neighboring devices and builds its local cache with information about these devices. A management workstation can retrieve this cache by sending SNMP requests to access the CDP MIB.

The format of the header is shown in the following illustration:

Version	TTL	Checksum	TLV	Type
1 byte	2 bytes	2 bytes	variable	2 bytes

CDP header structure

Version
The version of the protocol.

TTL
Time for this frame to live.

Checksum
Checks validity of previous fields.

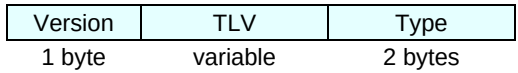
TLV
Contains a type, length and value field.

Type
1 Device ID.
2 Address.
3 Port ID.
4 Capabilities.
5 Version.
6 Platform.
7 IP Prefix.

DISL

Dynamic Inter-Switch Link protocol (DISL) synchronizes the configuration of two interconnected Fast Ethernet interfaces into an ISL trunk. DISL minimizes VLAN trunk configuration procedures because only one end of a link needs to be configured as a trunk. DISL is a Cisco protocol.

The format of the header is shown in the following illustration.



DISL header structure

Version

The version of the protocol.

TLV

Contains a type, length and value field.

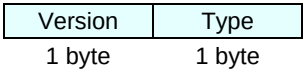
Type

1 Management Domain Name.
2 Status Field.

VTP

The VLAN Trunk Protocol (VTP) provides for each (router or LAN-switch) device to transmit advertisements in frames on its trunk ports. These advertisement frames are sent to a multicast address to be received by all neighboring devices (but they are not forwarded by normal bridging procedures). Such an advertisement lists the sending device's management domain, its configuration revision number, the VLANs which it knows about, and certain parameters for each known VLAN. By hearing these advertisements, all devices in the same management domain learn about any new VLANs now configured in the transmitting device. Using this method, a new VLAN needs to be created or configured on only one device in the management domain, and the information is automatically learned by all the other devices in the same management domain. VTP is a Cisco protocol.

The format of the VTP packet is shown in the following illustration:



VTP packet structure

Version

The version of the protocol.

Type

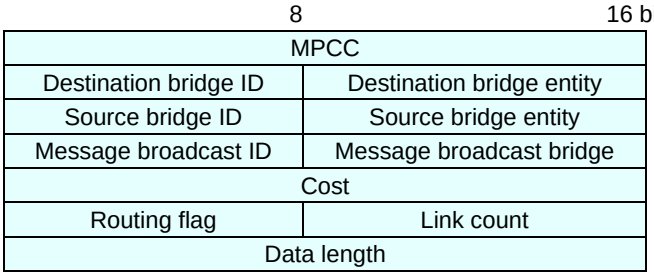
1 Summary- Advert Message.
2 Subset- Advert Message.
3 Advert-Request Message.

RND

RND Layer 2 Router Package Description 1993-04 1.00

The RND company produces communications equipment such as routers and bridges. The company uses a proprietary protocol header (known as RND) to transfer LAN protocols via WAN.

The structure of the RND header is shown in the following illustration:



RND header structure

MPCC

Specifies normal case or swap bytes case.

Destination bridge ID

Specifies the type of message:
0xF4 IPX router message.
0xF4 DECnet router message.
0xF7 IP router message.
0xF8 TRE management message.
0xF9 ETE management message.
0xFB Routing message bridge ID.
0xFC This bridge entity.
0xFD Channel status message.
0xFE Common LAN bridge ID.
0xFF Broadcast bridge ID.

Destination bridge entity
Value of the entity:
0x0F LAN broadcast entity.
0x64 Smap entity.
0x65 Reml entity.
0x6F C5 reml entity.
0x79 RS232 rem entity.

Source bridge ID
Refer to destination bridge ID above.

Source bridge entity
Refer to destination bridge entity above.

Message broadcast ID
0 Point-to-point.

Message broadcast bridge
0 Point-to-point.

Cost
Accumulated cost.

Routing flag
Routing attributes.

Link count
Count of router hops.

Data length
Length of the data in bytes (swapped).

Wellfleet SRB

Wellfleet, which is known today as Bay Networks, is a manufacturer of routers and bridges. They use a proprietary header in order to pass Token Ring information over WAN lines. This is known as Source Routing Bridging (SRB).

Destination	Source	Route information	LLC
6 bytes	6 bytes	variable & optional	variable

Wellfleet SRB structure

Destination

The address structure is as follows:

I/G	U/L	Address bits

Wellfleet destination address structure

I/G Individual/group address may be:
- 0 Individual address.
- 1 Group address.

U/L Universal/local address may be:
- 0 Universally administered.
- 1 Locally administered.

Source

The address structure is as follows:

RII	I/G	Address bits

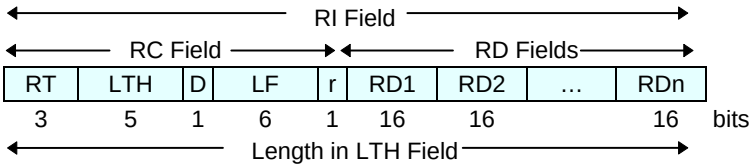
Wellfleet source address structure

RII Routing information indicator:
- 0 RI absent.
- 1 RI present.

I/G Individual/group address:
- 0 Group address.
- 1 Individual address.

Route information

The structure is as follows:



Wellfleet route information structure

RC Routing control (16 bits).

RDn Route descriptor.

RT Routing type.

LTH Length.

D Direction bit.

LF Largest frame.

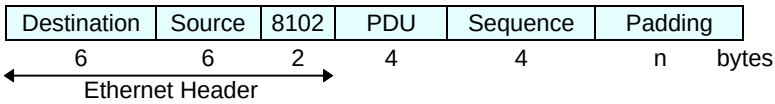
r Reserved.

Wellfleet BOFL

The Wellfleet Breath of Life (BOFL) protocol is used as a line sensing protocol on:

- Ethernet LANs to detect transmitter jams.
- Synchronous lines running WFLT STD protocols to determine if the line is up.
- Dial backup PPP lines.

The frame format of Wellfleet BOFL is shown following the Ethernet header in the following illustration:



Wellfleet BOFL structure

Destination
6-byte destination address.

Source
6-byte source address.

8102
EtherType (0x8102 for Wellfleet BOFL frames).

PDU
PDU field normally equals 0x01010000, but may equal 0x01011111 in some new releases on synchronous links.

Sequence
4-byte sequence field is an incremental counter.

Padding
Padding to fill out the frame to 64 bytes.

BPDU

IEEE 802.3D 1993-07, IEEE 802.1P 199

Bridge Protocol Data Unit (BPDU) is the IEEE 802.1d MAC Bridge Management protocol which is the standard implementation of STP (Spanning Tree Protocol). It uses the STP algorithm to insure that physical loops in the network topology do not result in logical looping of network traffic. Using one bridge configured as root for reference, the BPDU switches one of two bridges forming a network loop into standby mode, so that only one side of a potential loop passes traffic. By examining frequent 802.1d configuration updates, a bridge in the standby mode can switch automatically into the forward mode if the other bridge forming the loop fails.

The structure of the Configuration BPDU is shown in the following illustration:

	Octets
Protocol identifier	1-2
Protocol version identifier	3
BPDU type	4
Flags	5
Root identifier	6-13
Root path cost	14-17
Bridge identifier	18-25
Port identifier	26-27
Message age	28-29
Max age	30-31
Hello time	32-33
Forward delay	34-35

Configuration BPDU structure

Protocol identifier

Identifies the spanning tree algorithm and protocol.

Protocol version identifier

Identifies the protocol version.

BPDU type
Identifies the BPDU type: 00000000=Configuration, 10000000=Topology change notification. For the later type, no further fields are present.

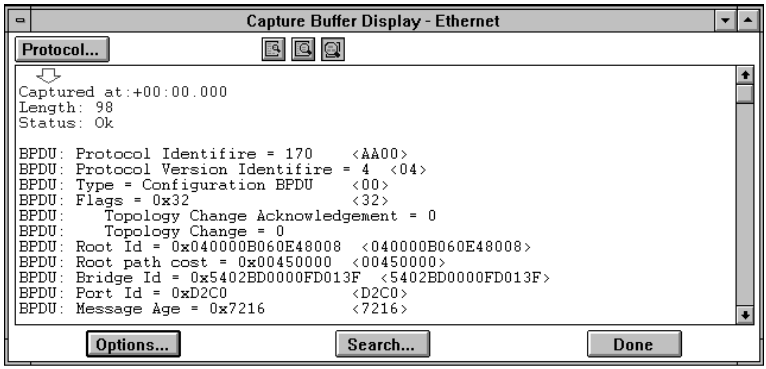
Flags
Bit 8 is the Topology Change Acknowledgement flag.
Bit 1 is the Topology Change flag.

Root path cost
Unsigned binary number which is a multiple of arbitrary cost units.

Bridge identifier
Unsigned binary number used for priority designation (lesser number denotes the bridge of the higher priority).

Port identifier
Unsigned binary number used as port priority (lesser number denotes higher priority).

Message age, Max age, Hello time, Forward delay
These are 4 timer values encoded in 2 octets. Each represents an unsigned binary number multiplied by a unit of time of 1/256 of a second. Thus times range from 0 to 256 seconds.



BPDU decode